TECHNICAL ADVISORY COUNSEL
A Subcommittee of the Commission on Technology
Minutes
November 22, 2002

Members Present:
Mohyeddin Abdulaziz
John Barrett
James Bondurant
Janet Cornell
Daniel Edwards
Karl Heckart
Carol Merfeld
Ellie Price
Kyle Rimel
Will Tagart

Members Not Present:
Ron Beguin
Sue Castaneda
David Davis
Joan Harphant

Others Present:
Jennifer Greene
Maureen Haggerty
Pam Peet

INTRODUCTIONS
Karl Heckart called the phone conference meeting to order at 9:30 a.m. and welcomed everyone attending.

Karl outlined the intent of the meeting was to discuss issues in preparation for formulating specific recommendations related to public access at the December meeting. Jennifer Greene summarized the recommendations from the Arizona Judicial Council's subcommittee, "Public Access to Electronic Court Records (PAECR)."

The key recommendations of a sensitive data form, a pilot and logging of document access were noted. The "pilot project" recommendation was discussed. Karl and Jennifer clarified that multiple court could participate. The pilot was focused at a three-year evaluation of the impacts, processes and procedures surrounding the provision of public access to criminal case documents.

Members discussed what courts are doing now in providing limited document access. Maricopa Superior provides minute entry access and wondered if this fell under the proposed rule. It was noted that though minute entries are technically considered a summary of proceedings, often judges embed orders of the court within them. If they are related to criminal cases and have "sensitive" information, then there may be some impact. Providing electronic documents pursuant to an email request was also brought up. Karl thought this was not the same as the registered access recommended and thought it likely that courts could do this if they wished.

The court expects the State Bar to respond to any rule changes related to these recommendations, especially the sensitive data form. PAECR had discussed that the impact of the recommendation would be to place the responsibility on attorneys (and/or

any filer) for not including sensitive data in a document and preparing the sensitive data form to accompany documents.

Mohyeddin noted that currently he limits access to parties in the case. Karl noted that this did not constitute the general public access that the PAECR focused on.

For a pilot, we need to decide what is viable and suggest parameters and processes that should be followed by any court participating in the pilot. Karl noted that the recommendations would have to go through a rules process (taking at least 6 months) and the sensitive data form would have to be developed. We would have sufficient time to develop a pilot program process.

Members discussed the recommendation of logging and tracking document access. Mohyeddin outlined his test of the process and referenced his email where he outlined the information available and some recommended processes. There was some concern about the impact of logging on performance.

Members discussed the need for the registration of users. Various approaches like credit cards, ID and passwords, and certificates were noted. A centralized registration and authentication site was generally thought to be the most reasonable approach. It was noted that e-filing, the case management system and the electronic document management system would all need to be integrated into this to provide for appropriate securing of documents. Mohyeddin offered to perform this registration service with his efiler software.

Janet suggested that we might learn from what other courts have done. It was noted that few have documents on-line. Karl will contact Colorado, where both the CMS and the EDMS is outsourced. We will follow up to see what the federal courts are doing but the preliminary report on their pilot is not due until September 2003.

Since the COT wants to know what's "doable" and what the costs and timeframes might be, members agreed we should concentrate on that. This included looking closely at the registration and logging recommendations.